RESEARCH PLAN PROPOSAL

Social Networking Sites and Cyber Crime:
(A Study of Deviance among Adolescents of Jaipur City)

For registration to the degree of
Doctor of Philosophy
IN THE FACULTY OF SOCIAL SCIENCES

THE IIS UNIVERSITY, JAIPUR

Submitted by
Pratibha Asudani
Enroll. No. IISU/2010/175

Under the Supervision of
Dr. Nisha Yadav
Professor & Head
Department of Sociology
The IIS University, Jaipur

Department of Sociology
The IIS University, Jaipur
November 2011

INDEX

S.No.	TITLE	Page No.
1	Introduction	1
2	Relevance of the Study	4
3	Review of Literature	5
4	Methodology	17
5	Limitations of the study	22
6	Chapter Scheme	23
7	Bibliography	24
	Annexure	I-IX

INTRODUCTION

The word cyber and its relative dot.com are probably the most commonly used terminologies of the modern era. We are now said to be in the midst of a 'new industrial revolution', one that will lead us into a new kind of society, a network society ,which has accelerated change and accentuated the qualities which have come to characterize late modernity. In the information society, the rapid development of computers, telecommunications and other technologies have led to the evolution of new forms of trans-national crimes known as "cyber crimes". Cyber crimes have virtually no boundaries and may affect any country in the world. They may be defined as, "any crime with the help of computer and telecommunication technology with the purpose of influencing the functioning of computer or the computer systems". The full social impact of cyberspace upon the individual is only just beginning to be understood. The extent of loss involved worldwide on account of cyber crimes is tremendous. It is estimated that about 500 million people who use the Internet can be affected by the emergence of cyber crimes. Cyber crime is a very serious threat for the times to come and poses one of the most difficult challenges before the law enforcement machinery. Most cyber crimes do not involve violence but rather greed, pride, or play on some character weakness of the victims. It is difficult to identify the culprit, as the net can be a vicious web of deceit and can be accessed from any part of the globe. To understand cyber crime as a significant new phenomenon, with potentially profoundly new consequences, it is necessary to recognize it as a constituent aspect of the wider political, social and economic restructuring currently affecting countries worldwide. This new technology not only provides opportunities for the profitable development of an international information market but has also raised the spectra of new criminal activities to exploit them. The

very technology that enables multinationals to do business more effectively and challenge the individual controls and regulations of nation states, also offers the prospect of globally organized criminal networks. Moreover the free flow of uncensored information on electronic networks and web- sites is as attractive to insurgents and extremist groups. Just as crimes have changed with the growth of information technology so have the categories of criminals who engage in such crimes. There are various categories of criminals who engage in such crimes, ranging from hackers, information merchants and mercenaries, to terrorists, extremists and deviants. The age group of these criminals varies from teenage to old age, varying with the nature of crime.

We live in an increasingly networked world. We are connected to each other through numerous types of ties, with social networking sites offering one of the most popular methods people currently employ to link themselves together. But do "old-fashioned" ways of developing and maintaining relationships suffer from the evolution of computer-mediated communication? Have we become too reliant on the instantaneous, answer-producing quality of the internet that can reveal others' most intimate personal details before we even introduce ourselves? Most of the Internet users are members of various social networking sites because of various reasons, without being aware of the harms it can have on their social life. It can lead to social isolation ,tension and conflict at individual, group and social life. It can also lead to various types of crimes such as cyber defamation, cyber bullying, creating organized clubs against some individual, state or even government. It can also create some terrorist organizations against some idea, region and religion.

The current study focuses on the magnitude of cyber crime by the extensive use of social networking sites and how it affects our society. It is widely held that the social environment has a profound impact upon how social interactions can take place (both licit and illicit), and in turn also gets affected by these which transforms the potential scope and scale of offending, altering the relationships between offenders and victims, and the potential for criminal justice

systems to offer satisfactory solutions. The “Time-Space compression” suggests that cyberspace makes possible near-instantaneous encounters and interactions between spatially distant actors, creating new forms of association and exchange which render us vulnerable. In addition, great emphasis is placed on how the Internet enables the manipulation and reinvention of social identity, adopting new virtual personae ,this is viewed as a powerful tool for the unscrupulous to perpetrate offences while maintaining anonymity through disguise.

Relevance of the study

The contemporary society is characterized by the extensive use of Internet. People of all age groups and strata have access to internet which on the one hand is giving them access to information but is also on the other hand giving them easy access to cyber criminal activities affecting the social fabric of society.

Increased use of Internet is leading to certain issues like destroying privacy, isolation, exposing children to online predators and a risk culture where even a small typing error can lead to online victimization. Today ,youngsters are using social networking sites indiscreetly, which apparently is affecting not only the pattern of social relations in present society but is also exposing them to associated risks.The current study aims to discover social implications of the use of social networking sites on the target group.

REVIEW OF LITERATURE

A literature review is a body of text that aims to review the critical points of current knowledge including substantive findings as well as theoretical and methodological contributions to a particular topic. Literature reviews are secondary sources, and as such, do not report any new or original experimental work.

Review of literature on Cyber crime is to find out what has already been done in this area, what type of theoretical explanations have been given about this new technological crime which is spreading very fast all over the globe, what have been the causes behind its occurrence and what effects it has on our society. Besides all this, it is also worthwhile to find out what laws and legislations are present to deal with this and what needs to be done in future for this.

Most Notable of the academic discourses about the social impact of technology were the long standing concerns expressed in the volumes on Industrial sociology from **Karl Marx**(1961).According to him, technology's function was perceived primarily as a means of rationalizing the power of capital by specializing the division of labor to reduce the cost of production process .As per the views of Marx, application of technologies of control alone tends to inscribe distrust into the process .In doing so it leads to the breakdown of trust relationships because they fail to reassure, create fresh demands for novel forms of trust and then institutionalizes them. In fact it seems that technologies of control can often make much worse the very problems they were designed to solve,

especially if in the case of spam, they end up hardening the spammer's resolve. There is evidence to show that the means of circumventing anti-spam measures is becoming more sophisticated and that there have been marked signs of resistance in the form of hactivism, denial of service attacks and various forms of hacking.

Weber(1958) wrote pessimistically of an 'Iron cage' of rationality and bureaucracy that will imprison us all. The same can be applied to crimes which have emerged in post-modern era. Rationality has caused more technical crimes. A move towards bureaucracies(a process which Ritzer (2002) has called McDonalization, whereby the principles of fast-food industry-efficiency, calculability, predictability and control-become increasingly applied to all forms of social life).As we experience changes in social environment, so all manner of new crimes and the spread of Information Technology brings with it new patterns of crime-from cyber crimes to mobile phone thefts. Cyber criminals have rational minds as most of them are technically sound, but instead of using it for social upliftment they involve in such acts with different motives behind them. Weber's conception of 'Ideal type' is quite applicable to the virtual environment created by cyberspace. As for weber, ideal types are considered as utopia or fantasy and on the other hand he told that ideal types were drawn from the reality itself.

Durkhiem(1951) viewed crime as an inevitable aspect of society, with uneven distribution of wealth and other differences among people. With industrialization came a wider and more intense Division of Labour as factory work came to be broken down into smaller repetitive tasks requiring less skills .the process of industrial production, also

spread geographically creating increasingly global levels of interdependence. The consequence of an expanding division of labor as discussed by Durkhiem saw, radical changes in old patterns of social relations .He describes this as a shift away from unthinking, habitual forms of mechanical solidarity ,towards an 'organic solidarity' rooted in the interdependencies created by Division of Labour. And though the latter was certainly much less personal and emotionally fulfilling for individuals, it was actually a more solid and systematic type of human interdependence that was capable of joining together the activities of people in geographically diverse communities (Cyberspace) and societies. Cyber crime is the result of this global interdependence. Sitting at on e corner of the globe, cyber crime can be committed in any other part without any physical or legal barriers which has given rise to cyber terrorism.

Merton(1968) examined anomie as a condition that occurs when discrepancies exist between societal goals and the means available for their achievement. This discrepancy or strain between aspirations and achievement has resulted in merton's conception being referred as strain theory. In reality the opportunities or means of achieving success are not available to all. This results in discrepancy between goals and means(strain) which produces various combinations of behavior in accepting or rejecting the means and goals.

One of the essential premises of this approach is that organization and disorganization in society are not mutually exclusive, but rather many of the cultural values that have desirable consequences (Manifest functions) often contain within them or produce undesirable consequences(Latent functions).Increase in technological upliftment has posed both manifest and latent functions .The use of Internet has been to send mails,

searching web, learning online etc but it is also used foe hacking ,pornography, bullying, spoofing etc.

Baudrillard(2003) describes the post-modern world as characterized by simulations; we live in the age of simulation. This process of simulations leads to creation of simulacra or “reproduction of objects or events”. With the distinction between signs and reality imploding, it is increasing difficult to tell the distinction between real and difficult. Example-In Software Piracy, illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original is done by end user copying, hard disk loading and illegal downloads from the internet. Eventually, it is the representations of the real, the simulations that come to be predominant. Baudrillard describes this world as hyperreality. Example-Spoofing, which makes one computer on a network to pretend to have identity of another computer, usually one with special access privileges. It becomes difficult to distinguish real from the spectacles.

Giddens(1991) has given dynamism to Modernity by three essential aspects of Gidden’s Structuration theory-Distanciation, Disembedding and Reflexivity, However, there are new and dangerous risks associated with modernity that always threaten our trust and leads to insecurity. Examples-The risk of crime caused by use of computers and internet has stem from globalised economy. People are not aware of these risks. It is these risks which give modernity the feeling of a runaway juggernaut and fill us with insecurity. Relationships with those who are physically absent and increasingly distant from us also lead to cyber crimes.

Jameson(2003) recognizes that postmodernism is usually associated with a radical break. He describes this new form as a cultural dominant. His concepts of Superficiality and lack of depth are relevant to cyberspace. Emergence of social networking sites coincide with superficiality as the people who are connected through these networks lack the basic connection and sentiments which are required for being human. Intensities occur when" body is plugged into the new electronic media". People are so much engulfed in surfing and chatting online that they forget about the real life .Internet also devours us of the man's past. Since it is impossible for users to find out the truth about each other's past, they have to rely on the information given.For the postmodern individual events are fragmented.

Beck(1992) examines the changing nature of society's relation to production and distribution is related to the environmental impact as a totalizing, globalizing economy based on scientific and technical knowledge becomes more central to social organization and social conflict. Beck labels the new ,or better yet newly emerging form as reflexive modernity. The contemporary world has elements of both industrial society and risk society, since many of those risks are traceable to industry which has also resulted in Globalization. A process of individualization has taken place in the west which has increased crimes. Due to complexity of society new crimes especially cyber crimes have come up which is again a risk for individuals, organizations and for state.

Ahuja(2000) explains various theories such as Differential Opportunity theory ,Differential Association theory, Strain theory, Space Transition theory which are very

much important for the study of cyber crime as these fit well with its occurrence. Cyber crime is white-collar as well professional crime because the individuals involved in it are technically sound as well as proficient. The Space transition theory clearly discusses the virtual space as an important element in the occurrence of new type of crimes.

Kshastri(2010) brings the fact that global cyber crime industry, which according to some estimates, is a US$1 trillion industry is growing rapidly. He examines economic and institutional processes in the cyber crime industry, provides insights into the entrepreneurial aspect of firms engaged in cyber-criminal activities, takes a close look at cyber crime business models, explains the global variation in the pattern of cyber crimes and seeks to understand threats and countermeasures taken by key actors in this industry.

Wall(2004) views Internet as one of the greatest sensations of recent times. It has become a symbol of our technological ingenuity and offers humankind an awesome array of benefits. However, the thrill of those prospects has been accompanied by public fears about the potential scale of criminal opportunities that can arise. Furthermore, there is clearly emerging a body of evidence to show that the criminal reality of the Internet is not the all engulfing “cyber-tsunami”, but, like the terrestrial world, a large range of frequently occurring small-impact crimes. One could argue that criminologists have been slow to explore these emerging fears and new criminal behaviors, and engage in debate about them in order to develop useful bodies of knowledge that could enlighten the public and provide the basis for informed policy. In

the criminologists' defense, however, it could be argued that there is wisdom in exercising caution and in waiting for reliable trends of behavior to emerge.

Mcquade(2008) observes " Whereas crime statistics of traditional types have been falling in recent years, cyber crime has exploded in an environment where traditional law enforcement has been largely unprepared. "*He* starts out with a valuable addition to the discussion of the sociology of cyber crime: the concept of deviance of behavior in a new and rapidly changing field. *The author also* reviews the various types of cyber attacks and crimes .The psychology of cyber criminals and abusers is reviewed which also provides a very detailed classification for social engineering, and Donn Parker's SKRAM (skill, knowledge, resources, access, motivation) model for assessing attackers. McQuade notes the difficulty in getting agreement on a profile for computer abusers, but does not address the changing style of attacks and attackers over time. Pornography, Hacking, Bullying, Cyberterrorism have been discussed by him in detail.

Jewkes(2006) analyses typologies of cyber crime in detail. He discusses on-line victimization, the social construction and policy implications of Internet crime, the dichotomous nature of cyberspace, the impenetrable anonymity of the virtual universe, and the challenges of regulation and control.

Ghosh(2010) has examined complex cyber crimes from the perspectives of multiple disciplines (computer science, law, sociology, psychology, etc.) and scientifically evaluate their impact on individuals, society, and nations holistically and

comprehensively. The author has addressed various issues as how multiple disciplines concurrently bring out the complex, subtle, and elusive nature of cyber crimes, how cyber crimes will affect every human endeavor, at the level of individuals, societies, and nations how to legislate proactive cyber laws, building on a fundamental grasp of computers and networking, and stop reacting to every new cyber attack, how conventional laws and traditional thinking fall short in protecting us from cyber crimes.

***Phair*(2007**) states "The Internet is not of the Wild West, as was once portrayed in American Western movies. It is just another public place and Internet users need to use real-world sensibilities when operating in the online environment." But his statement is quickly followed by a darker one of impending doom; "the communities trusting e-commerce activities, will slowly erode over time as personal users either become victims of online crime or know someone who has." He then briefly mentions 'the profile of cyber crime criminals' and how hacking the counterculture has completely changed into well-organized and hierarchical groups of criminal syndicates that have realized that there is substantial money to be made by criminal activity online.

Duggal((2009) provides a comprehensive overview of the cyber law scenario in India, provides recommendations for upgrading the current cyber law acts, and contextualizes these developments with respect to actual reported cases of cyber law in India. The author is a practicing advocate of the Supreme Court of India, and is a prolific writer and speaker. "Cyber law is important because it touches almost all aspects of transactions and activities concerning the Internet. Cyber law concerns everyone," Duggal begins. Drawing on the UNCITRAL law on e-commerce, the Indian government drafted the IT

Bill of 1999 which was then implemented as the IT Act 2000 in October 17, 2000. It targets three existing areas of la contract, penal code, and evidence, and expands the provisions of the Indian Penal Code of 1860, the Indian Evidence Act of 1872, the Banker's Book Evidence Act of 1891, the Reserve Bank of India Act of 1934, and the Companies Act of 1956. There are several positive aspects of the IT Act 2000: it provides legal infrastructure for e-commerce transactions, recognizes electronic documents as legal entities, opens up business opportunities for digital certificate companies, paves the way for e-government transactions, and creates provisions against cyber crime. The author calls for more education and orientation for police officers on the intricacies of cyber crime; there was a case of police officers carrying away computer monitors during a raid in Mumbai, thinking they were the actual computers.

Cross and Shinder(2002) analyses that law enforcement and IT security communities are now working diligently to develop the knowledge, skills, and tools to successfully investigate and prosecute Cyber crime cases. Over the past 5 years a great deal has changed in how computer crimes are perpetrated and subsequently investigated. Also, the IT security and law enforcement communities have dramatically improved their ability to deal with Cyber crime, largely as a result of increased spending and training. According to the 2006 Computer Security Institute's and FBI's joint Cyber crime report: 52% of companies reported unauthorized use of computer systems in the prior 12 months. Each of these incidents is a Cyber crime requiring a certain level of investigation and remediation. The contents also provide law enforcement officers with

an idea of some of the technical aspects of how cyber crimes are committed, and how technology can be used to track down and build a case against the criminals who commit them. It is now fairly established that the legal and technical landscape is need of the time to understand, prevent, detect, and successfully prosecute the criminal behavior that is as much a threat to the online community as "traditional" crime is to the neighborhoods in which we live.

Hawthorne & Klein(1999) talk about increasing use of women in creating a cyberculture which depict females as cyberbarbies and cyber sexobjects.The autors have also discussed Pornography in detail which is itself a social trauma.Pornography as one of the first successful e-commerce product has been the foremost crime on the internet.

Heuven & Botterman(2003) opines that attacks on computer networks have caused economic losses and created risks for national infrastructure security. In addition, criminals around the world are increasingly using computers to commit traditional crimes, such as financial fraud, distribution of child pornography, and copyright piracy .There is a need for increased consensus between the private sector, governments, and law enforcement officials to find the best means to counter hackers, computer virus spreaders, denial of service attacks, and use of the internet for illicit purposes .

Williams(2006) integrates theory and empiricism to forge an explanation of cybercrime whilst offering new insights into online regulation. The causes of cyber deviance, crime

and its control, as per Matthew Williams takes the Internet as a site of social and cultural (re)production, and acknowledges the importance of online social/cultural formations in the genesis and regulation of cyber deviance and crime.

The emphasis on criminal networks reflects a growing acknowledgment, among researchers into crime, that there is no single, dominant organizational structure with universal applicability, and the realization by law enforcement agencies that they are seeing patterns of organized crime that do not fit the traditional hierarchical structure is important to understand.

Richard Clarke, (2009), draws attention on Cyber terrorism which have the potential to reach out from cyberspace into the physical dimension, causing giant electrical generators to shred themselves, trains to derail, high-tension power-transmission lines to burn, gas pipelines to explode, aircraft to crash, weapons to malfunction, funds to disappear and enemy units to walk into ambushes. With cyber war, we have another means of launching attacks on the other side of the world, this time with only a keyboard.

METHODOLOGY

Operational definitions:

Cyber crime- Computer crime, or cybercrime, refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Such crimes may threaten a nation's security and financial health.

Social Networking site-is a site that enables users to create public profiles within that website and form relationships with other users of the same website who access their profile.Social networking sites can be used to describe community-based websites,online discussion forums,chatrooms and other social spaces online.

Deviance- in a sociological context describes actions or behaviors that violate cultural norms including formally-enacted rules (e.g., crime) as well as informal violations of social norms (e.g., rejecting folkways and mores).

Adolescents- the period between puberty and the completion of physical growth, roughly from 13 to 18 years of age. In this study students of 15-18 years of age-group will be studied.

Aims and Objectives

- To find out the extent and magnitude of cyber criminal activities in Jaipur city.
- To identify the socio-economic causes of Cyber crime .
- To analyze the impact of cyber crime on the victim and society.
- To comprehend Cyber crime vis-à-vis Levels of Income, Age, Gender and the duration of Internet Usage.
- To identify the impact of Social Networking websites on social life, academic performance and extra-curricular activities of younger generation.
- To assess the challenges that cyber crime presents for criminal justice systems and to review the measures taken by government to prevent cyber crime.
- To find out how much are youngsters aware of their privacy and safety on Internet.

HYPOTHESES

The research will be conducted on the basis of the following hypotheses.

1) It is hypothesized that Frequency and Intensity of using Social Networking Sites and deviance are significantly related..

2)The level of Income and Cyber crime are not significantly related.

3) Males/Young boys are more involved in committing Cyber crime as compared to females.

4) People in the age group of 25-35 are more prone to commit Cyber crime than people in other age groups.

Area, Universe and Sample

The area for the study is Jaipur city. Universe will consist of students in the age group of 15-18 years.

In the survey 500 respondents will be contacted for the purpose of data collection from five schools of jaipur city. For this purposive sampling will be used.

Tools for Data Collection

The following tools will be used for the purpose of the study:-

(1) **Questionnaire**-For the purpose of collecting first hand information and facilitating comparison of data a questionnaire will be prepared.

(2) **Unstructured Interview**-Due to the qualitative nature of the study it is assumed that besides the questions included in the questionnaire, certain supplementary questions will be asked.

(3**) Case Study**-Some case studies of people who have been the victims of cyber crime will be analyzed. This will help to assess the magnitude of cyber crime in society.

(4)**Secondary sources**-These sources help in providing certain information which may be difficult to obtain otherwise. Besides these sources also help in supplementing the information obtained through primary sources as well as providing guidelines to the investigator.

Data Analysis Tools

After collecting the data a descriptive analysis of the data will be done because it is both Qualitative as well as Quantitative which will be followed by an appropriate statistical analysis.

Statistical analysis will include tabulation of data and representation of data using graphs and charts for diagrammatic representation of data.

Correlation will be used to find out the relation between Cyber crime and levels of Income, Age, Gender and Time spent on Internet usage.

Limitations of the study

1. Limitations of time, space and manpower are the most restrictive aspects in an empirical study and the study may also be limited due to these aspects.

2. The answers of the respondents, as such will have to be taken as true.

3. The respondents may be quiet on certain issues and as such certain inferences will have to be drawn on the basis of observation of the overt behavior of the respondents which may include gestures and facial expressions.

4. The conclusions drawn may not be universal.

Chapter Scheme

(1) Cyber Crime and Indian Society: A Conceptual and Theoretical Framework.

(2) Social Networking Sites: Their Role in Contemporary India

(3) Review of Published Literature

(4) Methodology

(5) Cyber Crime in Jaipur city: Its Extent and Magnitude.

(6) Social Networking Sites and Deviance: An Empirical Study

(7) Conclusion

BIBLIOGRAPHY

Ahuja, Ram(2000). *Criminology*, Jaipur : Rawat Publications

Alexander, P.J(2002). *Cybercrime and Policing* ,Delhi:Allied Publishers.

Baudrillard, Jean (1994).*Simulacra and Simulation (The Body, In Theory: Histories of Cultural Materialism,* USA: The University of Michigan press.

Beck, Ulrich (1992). *Risk society Towards a New Modernity*, New Delhi: Sage Publications.

Blane,V.John(2003).*Cyber crime and Cyberterrorism*:*Current Issues*, New York :Novinka Books.

Brenner , W.Susan (2010). *Cybercrime:Criminal threats from cyberspace* ,Westport:Greenwood Publishing group.

Broadhust ,G.Roderic(2005).*Cybercrime:The challenge in Asia*, Hongkong:Hongkong University Press.

Chaubey,R K(2009).*An Introduction to Cyber Crime and Cyber Law* ,Newdelhi:Jain Book Depot.

Clough, Jonathan(2010). *Principles of Cybercrime*,Cambridge: Cambridge University press.

Colarik, M.Andrew(2006). *Cyberterrorism:Political and Economic Implications*, Denmark:Idea Group Publishers.

Duggal ,Pavan(2009).*Cyberlaw:The Indian Perspective*, New Delhi: Saakshar Law Publications.

Dasgupta, M(2009).*Cyber Crime in India*,New Delhi:Jain Book Depot.

Ghosh, Sumit (2010). *Cyber crimes: A Multidisciplinary Analysis*,New york:Springer Publications.

Giddens, Anthony(1990) .*The consequences of modernity*,California:Stanford University press.

Jameson ,Fredric(2003). *Postmodernism, or, The cultural logic of late capitalism*,USA:Duke University Press.

Jewkes ,Yvonne(2006).*Crime Online*, Canada: William Publishing.

Kshastri, Nir (2010).*The Global Cyber crime Industry*,USA:Springer Publications.

Martin, Clemans & Schell ,H.Bernodette(2004).*Cybercrime:A Reference handbook*,California:Polity Press.

McQuade,C.Samuel(2008).*Understanding and Managing cybercrime*,Boston:Allyn and Bacon.

Mehan, E.Julie(2008). *Cyberwar,Cyberterror,Cybercrime*,UK:IT Governance Publishing.

Milhorn ,H. Thomas(2007).*Cybercrime:How to avoid becoming a victim*, USA:Universal Publishers.

Phair,Nigel(2007) .*Cybercrime:The Reality of Threat*,E-Security Publishing.

Posey, Julie (2005).*My Life as a Cybercrime Fighter*,California:Polity Press.

Ritzer ,George(2007).*Sociological Theory,*New Delhi: McGraw-Hill Higher Education

Schmallcgen,Frank(2009).*Crimes of the Internet*,New Jersey:Prentice hall.

Shrivastava,Ashok(2005).*Indian Laws on Internet*,New Delhi:Jain Book Depot.

Thomas, Douglas (2000).*Cybercrime:Law Enforcement ,Security and Survelliance in the Information Age*,London: Routledge.

Verma, Amita(2009) .*Cyber Crimes and Law*,New Delhi: Jain Book Depot.

Wall, David(2004).*Cybercrimes and Internet,*New York: Barnes & Noble.

Wall, David(2007).*Crime and Society*,California: Polity Press.

Williams, Mathew(2006). *Virtually Criminal:Crime,deviance & regulation Online,*London:Routledge.

Yar, Majid(2006). *Cybercrime and Society* ,New Delhi:Sage Publications.

QUESTIONNAIRE
Social Networking Sites & Cyber Crime
(A Study of Deviance amongst Adolescents in Jaipur city)

NAME _____

AGE _____

GENDER _____

OWN A PC YES NO

INTERNET CONNECTION AT HOME YES NO

MEMBER OF A SNS YES NO

Q1) What is your main purpose of using Internet?

a)Educational

b)Entertainment

c)Communication

d)Research

Q2) What is the main cause of being user of a SNS?

a) Communication with friends

b) Educational Purpose

c) Exchange of Pictures and videos

d) Just for status

Q3) How frequently do you access your account on SNS?

a) Everyday

b) Once in a week

c) Once a fortnight

d) Once in a month

Q4) If you access your account everyday, how much time you spend on SNS?

a) Between 4-5 hrs b) Between 3-4 hrs

c) Between 2-3 hrs d) less than 2 hrs

Q5) From where do you access your SNS?

a) From Home b) From Cyber Café

c) From School d) Any Other

Q6) How many friends you have on SNS?

a) More than 50
b) Between 30-50
c) Between 10-30
d) Less than 10

Q7) How may SNS accounts you have?
a) Only one
b) between 2-10
c) Between 10-20
d) More than 20

Q8) Do you make friends who are unknown to you on SNS?
a) Yes
b) No

Q9) How much time you devote for your studies everyday?
a) More than 4 hrs
b) between 3-4 hrs
c) Between 2-3 hrs
d) Less than 2 hrs

Q10) How much time you spend on sports everyday?
a) Not everyday
b) Between 0-1 hrs
c) Between 1-2 hrs
d) More than 2 hrs

Q11) Do you participate in extra-curricular activities in school?
a) Yes
b) No
c) Sometimes

Q12) Do you share your problems with your friends on SNS?
a) Yes
b) No

Q13) Have you posted any personal information (telephone, address etc) on SNS?
a) Yes
b) No

Q14) Are you aware that your personal information can be misused through SNS?
a) Yes
b) No

Q15) Are your both parents working?
a) Yes
b) No

Q16) Do you feel good to go for family functions?

a) Yes b) No

c) Sometimes

Q17) Do you help your parents in house hold works?

a) Yes b) No

c) Sometimes

Q18) Do you feel free to communicate with your parents?

a) Yes b) No

c) Sometimes d) Depends on parent's mood

Q19) In your opinion, your parents like you being on SNS?

a) Yes b) No

c) Can't say d) They don't know about my membership on SNS

Q20) Do you reveal your friends on SNS to your parents?

a) Yes b) No

Q21) Under whose influence you joined SNS?

a) Siblings b) Peers

c) On your own d)Any other person

Q22) Do you feel the urge to check your account on SNS everyday?

a) Yes b) No

Q23) Do you share your personal pictures and videos through SNS?

a) Yes b) No

Q24) Have you ever come across a case of cyber defamation?

a) Yes b) No

Q25) Has someone bullied you on SNS?

a) Yes b) No

if yes, specify who? _____

Q26) Have you restricted access to your profiles so that only friends can view them?

a) Yes b) No

Q27) Are you aware of hacking through SNS?

a) Yes b) No

Q28) In your opinion why do users post fake information?

a) To protect themselves b) Just for fun

c) any other

Q29) Are you aware that online victimization can lead to offline setting which leads to physical victimization?

a) Yes b) No

Q30) Have you ever faced cyber bulling in any one of the form?

a) Receiving threatening messages b) Posting of embarrassing picture without permission

c) Spreading rumors online d) None of the above

Q31) Do you feel the need to use the SNS with increasing amounts of time in order to achieve satisfaction?

a) Yes b) No

Q32) Have you made effort to control cut back or stop SNS use?

a) Yes b) No

Q33) Do you use SNS's as a way of escaping from problems?

a) Yes b) No

Q34) Have you ever experienced at least one negative outcome as a result of using SNS?

a) Yes b) No

Q35) Are you aware of Identity-theft through SNS?

a) Yes b) No

Q36) Have you ever complained to your parents or teachers regarding something which you don't like on SNS?

a) Yes b) No

Q37) Do you feel like sending hate messages to your friends or teachers when you are angry with them?

a)Yes b)No

Q38)If given a chance ,will you like to hack someone's account on SNS ?

a)Yes b)No

Q39) Do you feel that online harassment is much easier as compared to Physical one?

a)Yes b)No

Q40) Do you feel that excessive use of SNS can lead to negative performance in studies?

a)Yes b)No

Q41) In your view, adolescents on SNS learn new abusive words?

a)Yes b)No

Q42) According to you what is the cause of cyber bulling?

a) Hatred b) Antagonism

c) Harrasment d)Show off

Q43) According to you what can be the cause of cyber defamation?

a) Failure in love b) Jealousy

c) any other

Q44) Do you feel blackmailing is much easier through SNS?

a) Yes b) No

Q45) What is the disadvantage of SNS?

a) Lack of face to face interaction b) Waste of time

c) Ground for cyber crimes d) addiction

e) all of the above

Q46) Do you feel that excessive use of SNS leads to negative physical health in adolescents? (Such as sleep disorders)

a) Yes b) No